UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/986,319	11/08/2001	Timothy J. Simms	16222.004	5579

23117 7590 03/17/2006

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/986,319	SIMMS, TIMOTHY J.
	Examiner	Art Unit
	Kaveh Abrishamkar	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 23 December 2005.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-3,5-9,24,26-31,36,38-56,112-123,127-143 and 149-151 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-3,5-9,24,26-31,36,38-56,112-123,127-143 and 149-151 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment received on December 23, 2005. Claims 1-3, 5-9, 24, 26-31, 36, 38-56, 112-123, 127-143, and 149-151 are currently being considered.

Response to Arguments

2. Applicant's arguments filed December 23, 2005 have been fully considered but they are not persuasive for the following reasons:

Regarding amended claim 1, the applicant argues that the CPA, Bellovin et al. (U.S. Patent No. 5,241,599), does not teach that "said first message being encoded with a symmetric encryption key" and "said second message being encoded with an asymmetric key." These arguments are not found persuasive. The CPA discloses that "Alice generates a random public/private key pair" and encrypts the public key or a portion thereof (random number) in a symmetric key cryptosystem (symmetric key) (column 5 lines 18-29). This is analogous to the first message being encoded with a symmetric key. Furthermore, the CPA states that "Bob generates a random secret key (R), and encrypts it in the asymmetric key cryptosystem" (column 5 lines 33-42). Therefore, it is respectfully asserted that the CPA does teach that "said first message being encoded with a symmetric encryption key" and "said second message being encoded with an asymmetric key" and the rejection is maintained and applied to the amended claims as given below.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1, 5-9, 18-19, 24, 26-31, 36, 39-40, 43-45, 47-51, 112-117, 120, 127-131, and 133-137 rejected under 35 U.S.C. 102(b) as being anticipated by Bellovin et al. (U.S. Patent No. 5,421,599).

With respect to claim 1, Bellovin et al. disclose a method for obtaining a shared secret key, comprising the steps of:

Identifying a first shared random number (column 6, lines 52-54, lines 62-67);

Identifying a second shared random number (column 6, lines 57-59; column 7, lines 2-10);

transmitting a first message from said second communicating party to said first communicating party, said first message including said first shared random number, and said first message being encoded with a symmetric encryption key (column 5 lines 18-29 column 6, lines 52-54, lines 62-67);

transmitting a second message from said first communicating party to said second communicating party, said second message including said second shared random number, and said second message being encoded with an asymmetric encryption key (column 5 lines 33-42), and

Obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number (column 7, lines 22-26).

4. With respect to claim 24, Bellovin et al. disclose a method for obtaining a shared secret key, comprising the steps of:

Receiving a first message including a first shared random number from said second communicating party, said first message being encoded with a symmetric encryption key (column 5 lines 18-29 column 6, lines 52-54, lines 62-67);

Identifying a second shared random number associated with said second communicating party, said first message being encoded with a symmetric encryption key (column 6, lines 57-59; column 7,lines 2-10);

transmitting a second message to said first communicating party, said second message including a second shared random number, and said second message being encoded with an asymmetric encryption key (column 5 lines 33-42)

Obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number (column 7, lines 22-26).

5. With respect to claim 112, Bellovin et al. disclose a method for obtaining a shared secret key, comprising the steps of:

Identifying a first shared random number associate with a first message from said second communicating party, said first message including a first shared random number, and said first message being encoded with a symmetric encryption key (column 5 lines 18-29 column 6, lines 52-54, lines 62-67);

Receiving a message including a second shared random number from said first communicating party, said second message being encoded with an asymmetric encryption key (column 5 lines 33-42, column 6, lines 57-59; column 7, lines 2-10); and

Obtaining a shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number (column 7, lines 22-26).

6. With respect to claim 5, Bellovin et al. disclose a method, further comprising the step of transmitting a second message from said second computer to said first computer, said second message including said second shared random number (column 6, lines 52-54, lines 62-67).

7. With respect to claim 26, Bellovin et al. disclose a method, wherein said step of identifying a second shared random number comprises generating said second shared

random number (column 6, lines 57-59; column 7, lines 2-10).

8. With respect to claim 113, Bellovin et al. disclose a method, further comprising the step of transmitting a first message including said first shared random number (column 6, lines 52-54, lines 62-67).

9. With respect to claim 133, Bellovin et al. disclose a method, further comprising receiving information identifying a user (column 5, lines 29-30).

10. With respect to claim 134, Bellovin et al, disclose a method, wherein said first key is associated with said user (column 5, lines 18-27).

11. With respect to claim 135, Bellovin et al. disclose a method, wherein said first key corresponds to a password known by said user (column 5, lines 18-27).

12. With respect to claims 6, 27, 28, 30, 39, 115, 118, 119, and 136, Bellovin et al. disclose a method, wherein said first message is encoded using a first key obtained using information obtained from a password. (column 5, lines 18-29; column 13, lines 18-20).

13. With respect to claims 7, 8, 29, 31, 40, 116, 120, and 137, Bellovin et al. disclose a method, wherein said step of encoding said first message comprises encrypting said

first message using said encoded password (column 5, lines 18-29; column 13, lines 18-20).

14. With respect to claim 9, Bellovin et al. disclose a method, wherein said first message also includes an asymmetric key (column 5, lines 18-29).

15. With respect to claims 49, and 117, Bellovin et al. disclose a method, wherein said first message also includes a second key (column 6, lines 52-54).

16. With respect to claim 50 Bellovin et al. disclose a method, wherein said second key is an asymmetric key (column 5, lines 18-29).

17. With respect to claim 51, Bellovin et al. disclose a method, wherein said second message is encoded using said asymmetric key (column 5, lines 33-41).

18. With respect to claims 36 and 43, Bellovin et al. disclose a method, further comprising receiving said password from a user (column 1, line 49).

19. With respect to claims 44 and 48, Bellovin et al. disclose a method, further comprising transmitting information identifying said user (column 1, line 46).

20. With respect to claim 45, Bellovin et al. disclose a method, wherein said user is a

human user (column 3, lines 13).

21. With respect to claim 47, Bellovin et al. disclose a method, further comprising decrypting said first message using information obtained from said password (column 5, lines 33-35).

22. With respect to claim 114, Bellovin et al, disclose a method, wherein said step of identifying a first shared random number comprises generating said first shared random number (column 6, lines 52-54, lines 62-67).

23. With respect to claim 127, Bellovin et al, disclose a method, further comprising decoding said second message (column 5, lines 42-45).

24. With respect to claim 128, Bellovin et al. disclose a method, wherein said decoding said second message comprises decoding said second message using a third key (column 5, lines 42-45).

25. With respect to claim 129, Bellovin et al. disclose a method, wherein said third key and said second key form an asymmetric key pair (column 5, lines 18-20).

26. With respect to claim 130, Bellovin et al. disclose a method, further comprising the step of generating said asymmetric key pair (column 5, lines 18-20).

27. With respect to claim 131, Bellovin et al, disclose a method, wherein said asymmetric key pair is generated dynamically (column 5, lines 18-20).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

28. Claims 2, 3, 38, 52, 122, and 123 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin et al. (U.S. Patent 5,241,599) in view of Shona et al. (U.S. Patent 6,018,581).

29. Bellovin et al. and Shona et al. are analogous art because both are in the field of electronic communication.

30. With respect to claim 2, and 122, Bellovin et al. does not disclose a method, wherein said combining function includes a logical function. Shona et al. disclose a method,

wherein said combining function includes a logical function (column 6, lines 12-16, lines 22-25).

31. It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Shona et al. with the teachings of Bellovin et al. in order to make the encryption key greatly varied (column 6, lines 25-29).

32. With respect to claim 3, 38, and 123, Bellovin et al. does not disclose a method, wherein said logical function includes an exclusive or (XOR) function. Shona et al. disclose a method, wherein said logical function includes an exclusive or (XOR) function (column 6, lines 12-16, lines 22-25).

33. The motivation for combining the teachings of Shona et al. with the teachings of Bellovin et al, is disclosed above.

34. With respect to claim 52, Bellovin et al. disclose a method of claim 37, wherein said second message is encrypted with said second key (column 5, lines 33-41).

35. Claims 41, 42, 46, 138-141 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin et al. (U.S. Patent 5,241,599) in view of Wu (U.S. Patent 6,539,749).

36. Bellovin et al. and Wu are analogous art because both are in the field of electronic communication.

37. With respect to claim 17, Bellovin et al. disclose a signal (column 5, lines 10-11: The communication is conducted over telephone lines, meaning that data must be transmitted through a continuous transmission signal.

38. Bellovin et al. do not disclose a signal wherein said signal comprises a packet of data representing a portion of said information.
Wu discloses a signal, wherein said signal comprises a packet of data representing a portion of said information (column 3, lines 62-63 : If one has the ability to intercept packets that make up messages transmitted from one person to another on the network, that necessarily means packets of information are used to represent a portion of information.

39. It would have been obvious to one of ordinary skill to combine the teachings of Wu with the teachings of Bellovin et al. because it is well known in the art to send information over a data network through packets.

40. With respect to claim 41, Bellovin et al. do not disclose a method, wherein said encrypted password is obtained from an output of a one-way function having an input including said password.

Wu discloses a method, wherein said encrypted password is obtained from an output of a one-way function having an input including said password (column 5, lines 48-52).

41. It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Wu with the teachings of Bellovin et al. in order to enable the server which the user is trying to access to determine if the user knows the password for the account specified during login (column 5, lines 42-45).

42. With respect to claim 42, Bellovin et al. do not disclose a method, wherein said one-way function is a hash function.

Wu discloses a method, wherein said one-way function is a hash function (column 5, lines 48-52).

43. The motivational benefits of combining the teachings of Wu with the teachings of Bellovin et al. are disclosed above.

44. With respect to claims 46 and 138, Bellovin et al. do not disclose a method, further comprising the step of obtaining said first key from an output of a one-way function having an input including said password.

Wu discloses a method, further comprising the step of obtaining said first key from an output of a one-way function having an input including said password (column 5, lines 42-45).

45. The motivational benefits of combining the teachings of Wu with the teachings of Bellovin et al. are disclosed above.

46. With respect to claim 139, Bellovin et al, do not disclose a method, further comprising the step of obtaining said first key by looking up said user in a password file. Wu discloses a method, further comprising the step of obtaining said first key by looking up said user in a password file (column 3, lines 33-37).

47. It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Wu with the teachings of Bellovin et al. in order to verify that the user asking to log onto a server is who the person claims to be (column 3, lines 23-25).

48. With respect to claim 140, Bellovin et al, do not disclose a method, wherein said password file contains an encoded password.
Wu discloses a method, wherein said password file contains an encoded password (column 3, lines 33-37).

49. It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Wu with the teachings of Bellovin et al. in order to verify a user's asserted password without having to reveal the user's password

(column 3, lines 35-37).

50. With respect to claim 141, Bellovin et al. do not disclose a method, wherein said encoded password is an encrypted password.

Wu discloses a method, wherein said encoded password is an encrypted password (column 3, lines 33-37).

51. The motivational benefits of combining the teachings of Wu with the teachings of Bellovin et al. are disclosed above.

52. Claims 142 and 143 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin et al. (U.S. Patent 5,241,599) and Wu (U.S. Patent 6,539,479) in view of Kung et al. (U.S. Patent 5,434,918).

53. Bellovin et al., Wu, and Kung et al. are all analogous art because all are in the field of electronic communications.

54. With respect to claim 142, Bellovin et al. and Wu do not disclose a method, wherein said password file is encoded.

Kung et al. disclose a method, wherein said password file is encoded (column 3, lines 2629).

55. It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Kung et al. with the combined teachings of Bellovin et al, and Wu in order to protect the password file (column 3, line 24).

56. With respect to claim 143, Bellovin et al. and Wu do not disclose a method, wherein said encoded password file is an encrypted password file. Kung et al. disclose a method, wherein said encoded password file is an encrypted password file (column 3, lines 26-29).

57. The motivational benefits of combining the teachings of Kung et al. with the combined teachings of Bellovin et al. and Wu are disclosed above.

58. Claims 54-56, 132, and 149-151are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin et al. (U.S. Patent 5,241,599) in view of Gutowitz (U.S. Patent 5,365,589).

59. Bellovin et al. and Gutowitz are analogous art because both are in the field of electronic communication.

60. With respect to claims 54 and 149, Bellovin et al. do not disclose a method, wherein said first message also includes a timestamp. Gutowitz discloses a method, wherein said first message also includes a timestamp (column 32, lines 31-34).

61. It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Gutowitz with the teachings of Bellovin et al. in order to provide application-specific parameters so as not to redundantly send information (column 32, lines 18-37).

62. With respect to claims 55 and 150, Bellovin et al, disclose a method, wherein said first message also includes a second key (column 6, lines 52-54).

63. Bellovin et al. do not disclose a method, wherein said first message also includes a timestamp. Gutowitz discloses a method, wherein said first message also includes a timestamp (column 32, lines 31-34).

64. The motivational benefits of combining the teachings of Gutowitz with the teachings of Bellovin et al. are disclosed above.

65. With respect to claims 56 and 151, Bellovin et al. disclose a method, wherein said second key is an asymmetric key (column 5, lines 18-29).

66. With respect to claim 132, Bellovin et al. do not disclose a method,'wherein said asymmetric key pair is selected from a set of pre-generated asymmetric key pairs. Gutowitz discloses a method, wherein said asymmetric key pair is selected from a set of pre-generated asymmetric key pairs (Abstract, lines 10-12; column 3, lines 59-60).

132. It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Gutowitz with the teachings of Bellovin et al. in order to make code breaking and tampering with the encryption more difficult (column 3, lines 54-60).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

KA
03/13/2006